UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/736,717	12/12/2000	David Michael Kurn	20206-036 (P00-3418)	8320

7590 12/19/2005

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/736,717	KURN ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Minor Informalities

1. The Applicant is required to submit a clean copy of the claims, because the claims submitted 11/17/2005 contain a line through the claims. Substitute claims are required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 13-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. More specifically claims 17-18, which depend from claim 13, are rejected under 112 1st for the limitations of "key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users". In the specification on page 15 lines 10-17, there is not disclosed, "key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users". On page 15 there is a disclosed an integrity key that is used to protect the database and a protection key used to protect the data in the database. There is a disclosed what makes up the integrity key and protection key; however there is not disclosed "key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users".

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

5. Claims 13-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. More specifically claims 17-18, which depend on claim 13, are rejected under 112 2nd for claiming new matter. Claim 17, claims, "key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users". There is not disclosed, "key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users". On page 29 lines 1-20 of the specification, disclosed each owner key is constructed and split using Bloom-Shamir. Claims 17 contain new matter that will not be examined, because it is not disclosed in the specification.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-12, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot(6,317,829) in view of Eastlake and further in view of Okamoto et al(6,118,874).

8. As per claims 1, 11, 21 , Van Oorschot discloses a cryptographic keys used during operation of a computer system(see col. 3, lines 20-24), providing an old set of cryptographic keys(see col. 6, lines 21-32, col. 7, lines 3-14); including at least a first cryptographic key protects an integrity of secret information stored in a database(see col. 6, lines 33-47), and the second cryptographic key protects access to the secret information stored in the database(see col. 4, lines 52-58, col. 7, lines 30-41), checking with a key repository to determine if a certificate re-issuance is necessary, meanwhile maintaining the availability of the old set of cryptographic keys(see col. 6, lines 22-32, col. 7, lines 3-14); the new keys are stored in the database(see col. 4, lines 24-48, col. 7, lines 6-11), providing the new or revised keys to applications that need them when next requested by such applications(see col. 3, lines 30-39, col. 6, lines 22-32). Van Oorschot discloses an application, because the primary computing unit, and the server communicated the key history information via a internet link(see col. 5, lines 3-6), an application is inherent in Van Oorschot, because Van Oorschot discloses communicating the key information to the primary computing device via an Internet link, this link has an application, such as a web browser. However, Van Oorschot does not disclose key rollover. Eastlake does disclose key rollover.

9. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Van Oorschot with Eastlake to include key rollover, one would have been motivated to include key rollover of Eastlake, because in order to obtain high levels of security, keys must be periodically changed, or "rolled over"(see pg. 3 of Eastlake). Rollover is necessary because the longer a private key is used the more likely it is to be compromised due to cryptanalysis, accident or treachery(see pg. 3 of Eastlake).

10. Neither Oorschot nor Eastlake disclose wherein the applications detect a missing key, and check with the key repository for the missing key, and if the missing key has been reissued, the applications receive the reissued key. Okamoto discloses wherein the applications detect a missing key, and check with the key repository for the missing key, and if the missing key has been reissued, the applications receive the reissued key(see fig., 8, sheet 9, and associated descriptions). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Van Oorschot-Eastlake combination with Okamoto to include wherein the applications detect a missing key, and check with the key repository for the missing key, and if the missing key has been reissued, the applications receive the reissued key, one would have been motivated because there is the possibility that secret information cannot be recovered because of a key being lost or the owner of a key becoming unavailable(see col. 2, lines 28-31 of Okamoto). It is an economical loss whenever the secret information that cannot be recovered is used in the activity of an enterprise(see col. 2, lines 31-33). One effective approach is to provide a key recovery system in which a copy of a key is backed up so that the key can be recovered(see col. 2, lines 33-36 of Okamoto).

11. As per claim 2, Van Oorschot discloses key repository utilizing one or more services of a specialized application acting as an extension of the key repository (col. 3, lines 27-39, col. 6, lines 22-32).

12. As per claim 3, Van Oorschot discloses the key repository utilizes the one or more services of the specialized application, authenticating authorization of the specialized application to perform one or more services(see col. 3, lines 27-39, 51-67, col. 7, lines 30-53).

13. As per claim 4, Van Oorschot discloses a command that when the key is about to approach expiration, a new key is issued(see col. 6, lines 22-32). Van Oorschot does not disclose invoking the command. Eastlake discloses invoking a key rollover. The motivation to include invoking the key rollover, is that being invoked as a result of a command, is the longer a private key is used, the more likely it is to be compromised due to cryptanalysis, accident or treachery(see pg. 3 of Eastlake).

14. As per claim 5, Van Oorschot discloses a periodic check which senses that the old set of cryptographic keys are approaching expiration (see col. 4, lines 24-47, col. 6, lines 21-32).

15. As per claim 6, Van Oorschot discloses a result of sensing an expired key(see col. 4, lines 24-47, col. 6, lines 21-32).

16. As per claim 7, Van Oorschot discloses wherein the applications are notified of the presence of new keys by the key repository process(see col. 8, lines 41-56).

17. As per claim 9, Van Oorschot discloses wherein the key repository process is prompted by the applications to invoke the method as a result of the applications detecting a key approaching expiration (see col. 6, lines 62-67, col. 7, lines 1-11).

18. As per claim 10, Van Oorschot discloses wherein the applications request the key repository process to provide a new key as a result of applications detecting an expired key(see col. 7, lines 1-14).

19. As per claim 11, Van Oorschot discloses a key repository configured to maintain at least a first key and second key(see fig. 1, sheet 1), and a database coupled to the key repository(see fig. 1, sheet 1), and storing secret information wherein the first key protects an integrity of the

secret information stored in the database(see col. 6, lines 33-49), and the second key protects access to the secret information stored in the database(see col. 4, lines 52-58, col. 7, lines 30-41).

20. As per claim 12, Van Oorschot discloses at least one application that can access the key repository, wherein the at least one application is preauthorized to access the second key and can perform at least one function using the secret information without user intervention(see col. 5, lines 64-67, col. 6, lines 1-7).

21. As per claim 21, limitations have already been addressed(see claim 1, and 11).

22. Claims 13-20 are rejected under 112 1st, because the claimed limitations are not described in the specification.

Response to Amendment

21. As per claims 8, and 21, previously indicated as allowable, has been withdrawn. The Examiner has found art to reject the limitations of these claims.

22. The Examiner also rejected claims 13-20 under 112 1st. The Applicant provided citations in the specification were the claim limitations were found. However, the Examiner still does not see how claim 17 is taught in the specification. The Examiner read the citations provided, but still does not see the claim limitations taught. Therefore, the rejection under 112 1st still stands, and further claim 17 is rejected under 112 2nd(see above for remarks).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

December 8, 2005

Primary Examiner
AU 2131
12/14/05